PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G06F 1/00

A2

(11) International Publication Number: WO 00/67096

(43) International Publication Date: 9 November 2000 (09.11.00)

(21) International Application Number: PCT/US00/11997

(22) International Filing Date: 3 May 2000 (03.05.00)

(30) Priority Data:
09/304,245 3 May 1999 (03.05.99) US

(71)(72) Applicant and Inventor: CALAMARI–LINDQUIST, Eleanor (aka ST. JOHN, El) [US/US]; Silvertech Inc., Suite 103, 1415 Indiana Street, San Francisco, CA 94107 (US).

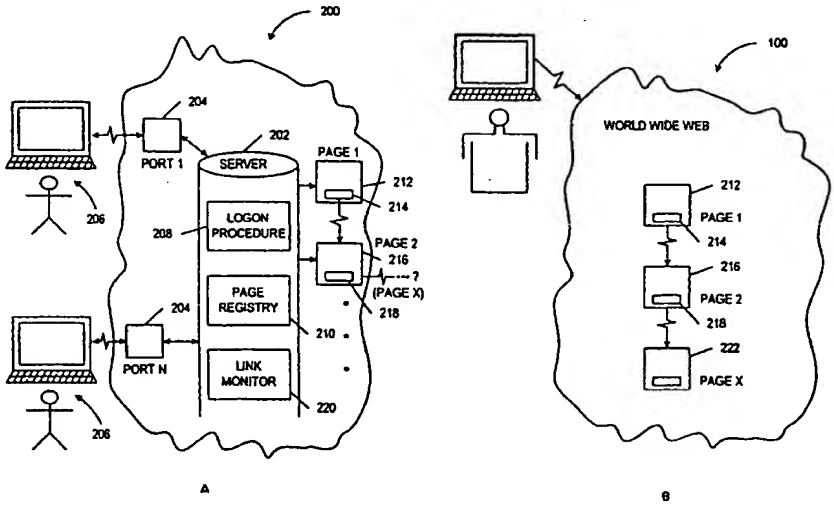
(74) Agent: IVEY, James, D.; Law Offices of James D. Ivey, 3025 Totterdell Street, Oakland, CA 94611–1742 (US).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: INTERNETWORKING SYSTEM FOR PROVIDING SAFE AND SECURE ACCESS FOR PRIVATE GROUPS



(57) Abstract

A system is presented for providing a secure and safe internetworking system that is a completely self–contained internet exclusively for children or other private groups. The system comprises a server system, a plurality of dial–up ports connected to said server system, and a plurality of web pages comprising content that is suitable for children or other private groups. The address space of content loaded onto the system may be partitioned for individual children or member and may be increased by authenticated, verified consent by parents or system administrators. The system provides hardware and/or means for authorizing the addition of requested web pages onto the system. In another aspect of the present invention, there is an upper limit imposed on the number of children engaged in any particular chat room. Chat among children is monitored either by humans or automatic language filters whereby the number of children in a given chat room does not exceed a pre–set upper bound.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNETWORKING SYSTEM FOR PROVIDING SAFE AND SECURE ACCESS FOR PRIVATE GROUPS

FIELD OF THE INVENTION

The present invention relates to an internetworking system in general and, in particular, to an internetworking system characterized by a safe and secure access for select groups of individuals.

BACKGROUND OF THE INVENTION

In recent years, the Internet has proliferated -- approximating a truly ubiquitous medium of communication for all people. Indeed, notions of "universal" access to the Internet have become intertwined with the notions of basic fairness and accessibility for all people - regardless of income, race, physical disability or location. Thus, it is not uncommon to find Internet access in public places - e.g. schools, libraries, etc. - available to the general public at little or no cost.

This unrestrained universality of access to the Internet has conflicted in a myriad of ways with notions of privacy. Questions such as: how much information regarding private lives should be available on the Internet; how much regulation should be placed on an individual's time, place and manner of use of - as well as an individual's speech on -the Internet; how much security - in terms of encryption (weak or strong) - should be available to the general public; and whether the government has a compelling right or interest in monitoring private conversations; has been the subject of much debate and growing legislation.

One class of citizenry in the United States has warranted singling out for special protection - children. Indeed, "[k]ids are a particularly vulnerable audience", noted the chairman of the Federal Trade Commission, Mr. Robert Pitofsky, as the FTC proposed new rules implementing the Children's Online Privacy Protection Act of 1998. (c.f. "U.S. Urges New Rules to Guard Privacy of Children on Internet", New York Times, April 2 1, 1999.) The Privacy Protection Act recognizes that kids are easy prey for marketeers, as it requires that

proprietors of commercial Web sites obtain parental consent before seeking personal information from children. The new rules require companies to obtain ,'verifiable parental consent" through a variety of means, such as, post card, facsimile, email, or digital signatures.

The problem with the above-listed means is that each in their own way may be thwarted - either by companies or by the children themselves. For example, unscrupulous companies may blatantly disregard the rules; or children may easily disguise their actions as those of their parents; thereby giving a false consent. It is thus widely acknowledged that without strong verification and enforcement mechanisms in place, "the rules are an empty gesture", according to Mr. Pitofsky.

The difficulties and dangers that confront children on the Internet, however, do not stop with aggressive marketeering. Indeed, well-documented predatory practices of pedophiles include: conversing with children on-line (e.g. in chat rooms) and possibly disguising one's true age, sex or some other characteristic in order to entice the child into an actual meeting. Sadly, kidnappings, sexual molestation, or other such acts represent the darker side to the Internet for young children who suffer the misfortune of having their fates intertwined with such elements of society.

As a response to this need to provide a "safe haven" for children, some Web sites (e.g. Headbone Zone, Kids Club, Child.net, Free Zone, among others) have sprung up that purport to offer such a safe and secure place. These sites host, by and large, material and content that is suitable for children. In addition, some of these sites provide chat rooms in which kids may converse in a monitored, safe environment. (c.f. "Keeping the Internet Safe for Young Chatters", New York Times, November 5, 1998). Monitoring of these sites are typically accomplished in one of two fashions - automatic language filters or human monitors. Monitors, either human or automatic, review the language of the posts of the children in the chat rooms; and, if any child posts inappropriate or obscene language, that child is subject to a variety of potential sanctions. Such sanctions may be anywhere within the range of a warning to being logged-out or having their accounts canceled. Other rules that are typically enforced in these monitored chat rooms include forbidding the exchange of last names, non-site email address, names of schools or hometowns, ZIP codes, phone numbers, or any other information between chatters that might facilitate an off-line meeting.

The common problem shared among the above-mentioned sites is security. These sites require that the child access their dedicated web site through, typically, the child's parent's account on the World Wide Web - thus, allowing the child the opportunity to be exposed to the entire Internet and all its attendant dangers. Figure 1 depicts the typical such environment

as encountered by children who access the World Wide Web through an internet service provider's (ISP) account. World Wide Web 100 comprises numerous sites accessible to those children 102 and adults 104 who have accounts on ISPs 106. Child 102 typically logins into ISP 106 via his or her parent's account. From the ISP, it is the parent's fervent hope that their child will head to a designated child friendly site 108 -with all of its appropriately targeted content for young viewers -- and not to the multitude of adults-only sites 110 that pervade the Web.

Once inside the child friendly site, the child may browse freely through its materials, or enter one or more chat rooms 112 that are hosted by the child friendly site. There, the child might converse with other children, possibly in a monitored chat room where an adult (not shown) checks the appropriateness of the language of the children and metes out the appropriate sanctions for breaches.

However, as the child entered the child friendly site via the World Wide Web, there is generally no guarantee that the child may not access other sites on the Web, including an adults-only site] 10. Once outside the protective cover of the child friendly site, the child is potentially exposed to chance encounters with unscrupulous individuals (including pedophiles) who might seek to do harm to the child. These encounters might happen in other chat rooms 114 that are associated with these other sites on the Web. Generally speaking, there is no monitoring of language and behavior in these chat rooms for the protection of children.

Aside from the lack of barriers to children surfing the entire Web in general, another pressure on child safety appears to derive from the Privacy Protection Act of 1998 - the same Act that purports to protect children. As mentioned above, the Act requires that the sites obtain permission from the parent before a child may gain access to a site that is intended to be child friendly. Thus, the Act may have the "unintended consequence [of] pushing children into sites meant for more mature audiences, because it will be cumbersome for them to get [parental] permission to view some children's sites." (c.f. "New Serious Side to Child's Play on Web", New York Times, November 26,1998).

Apart from the special needs of children, broader notions of safety, security and a sense of community are also germane to other, private groups of individuals. For example, doctors, lawyers, accountants and other professional persons might find a private internet having the same level of protections and community desirable.

Thus, there is a need for an Internetwork system that gives children relatively easy access to children sites - while obviating the possibility that children may have access to adult

sites.

There is another need for a system that minimizes the possibility of an adult, posing as a child, in order to gain access to children's chat rooms for potential harmful results.

There is yet another need for a system that allows for seamless integration of child-related content, presented in a fun and educational manner to children.

There is still another need for producers and suppliers of child-related content to distribute their value-added products or services to children in a seamless fashion that also conforms to the dictates of the Privacy Protection Act.

There is still yet another need for groups of private individuals having a common set of goals or interests to have a secure internetworking system that comprises relevant content to that particular group. Such content is not necessary limited to that produced from one company; but may be chosen from a wide variety of sources relevant to the particular dictates and goals of the group.

There is still another need for such a private internetworking system to allow members to request loading information from other sources onto the private system.

SUMMARY OF THE INVENTION

The present invention meets the aforementioned needs by providing a secure and safe internetworking system that is a completely self-contained internet exclusively for children or other private groups. In one aspect of the presently claimed invention, the system comprises a server system, a plurality of dial-up ports connected to said server system, and a plurality of web pages comprising content that is suitable for children or other private groups.

In operation, parents of children would initially subscribe their child to the system and each child, in turn, would be issued a login account. The child would dial into the system via its dedicated dial-up ports and would engage in a login procedure. After proper authorization, the child would be free to browse around inside the presently claimed system, accessing pre-approved web pages that have been installed on the server system.

The web pages might preferably comprise copies of web pages that are actually found on World Wild Web and, thus, may contain hypertext links to other web sites embedded within the web page.

The child would be able to make requests to jump to any hypertext link found in any web page. Whether the child receives the requested page depends upon whether the requested

page has been loaded onto the server system. If the requested page is installed, then the child's browser would download and exhibit the page in question. Otherwise, the child's browser might inform the child that the requested page has not yet been authorized for access on the system.

Alternatively, the system might engage in a search for approved sites already loaded onto the server that are similar in content to the unapproved requested site. In yet another alternative, the web pages loaded onto the server may have its embedded links pre-screened and edited out, if it is deemed that the site being linked to is inappropriate for the target audience.

In another aspect of the presently claimed invention, the system would provide hardware and/or means for authorizing the addition of requested web pages onto the system. For example, if the requested pages contain content that is deemed suitable for older teenagers; but not necessarily for young children, then the system might inform the parents of the child of the child's request for additional web pages. The parents might then review the requested pages and decide whether their child should have access to the requested pages. Authentication hardware and/or means is supplied by the present invention whereby parental consent could be given to the system to upload and link the additionally requested pages onto the system for their child to view. Thus, the presently claimed system could either make these added pages either globally accessible to all account on the kids-internet; or, it might maintain a registry of allowable web pages for each individual child or subsets of children. Alternatively, web pages could be classified according to the age group each is suited for -- "under 6 years old", "6 to 8 years old", etc. Each child's account could contain information about the highest age group the child's parents want the child to see.

In another aspect of the present invention, there is an upper limit imposed on the number of children engaged in any particular chat room. Chat among children is monitored either by humans or automatic language filters whereby the number of children in a given chat room does not exceed ten children. Preferably, chat rooms are monitored by humans where chat room enrollment is limited to no more than four children.

The above aspects of the present invention are applicable to not only children; but to groups of private individual who share a common set of goals or sense of community. Content on such a private internet may be pre-approved and mechanisms in place for the requesting and porting of other content onto the system are germane aspects of the present invention. Additionally, chat rooms, private email, and other means of communication fosters a sense of community among members of the private internet.

One advantage of the present invention is enhanced safety and security. The child, by virtue having his or her own account, is allowed to browse in a relatively self-contained virtual environment. The presently claimed system does not connect, in general, to the greater World Wide Web; and, as such, children are not able to retrieve web pages of questionable content.

Additionally, as the presently claimed system is accessible only by subscription, no outside individuals are generally able to engage in chat or other contact with the subscribing children.

Another advantage of the present invention is manageability. Chat rooms in the presently claimed system has an imposed upper limit of children; making the task of monitoring and refereeing chat effective to check the natural tendency of children to test the limits of the imposed rules in the system.

Another advantage of the present invention is that subscribers always stay on the self-contained network, rather than going from the network to sites on the public Internet that are owned and operated by other companies. This enables the designer of the self-contained network to provide a consistent interface to the user, making the network easier to use and helping to build a sense of community among subscribers. It also means that the self-contained network is a "sticky" site, to use a term applied to websites on the public Internet. In evaluating the popularity of websites on the public Internet, two key factors are how many "hits" the site receives (i.e., how many users visit the site), and how long users stay at that site before they go elsewhere on the Internet. A "sticky" site is one that users tends to stay at for a relatively long period of time. The present invention is directed at an extremely "sticky" site, since subscribers always remain within the self-contained network when using the network, even when it appears that they are visiting other sites on the public Internet.

Yet another advantage of the present invention is speed and ease-of-use. Because the private network contains a vast amount of content that has already been downloaded from the Internet, subscribers are able to access this information more quickly and with greater ease than if they had to separately find and connect all of this information on the public Internet.

Although the claimed system is especially suitable for providing a self-contained, secure networking environment for children, it can be advantageously used in other contexts as well. Security is a significant concern for any individual or company that uses the Internet. When a user accesses the Internet, the user is vulnerable to unscrupulous individuals who may try to use the user's link to the Internet to gain access to the user's individual computer files. In addition, harmful computer viruses may be rapidly spread across the Internet, as evidenced by

the recent "Melissa" virus. A self-contained, private network is less susceptible to these threats, since access is limited to subscribers, and the network consists of private servers that are not connected to the public Internet. Although a self-contained network is not immune to such threats, it is easier to implement security measures on a private network than on the public Internet.

Similarly, speed and ease-of-use are also significant considerations for any individual or company that uses the Internet. Although the Internet contains a vast amount of useful information on a virtually unlimited number of subjects, it can be difficult and time-consuming to locate pertinent information on a particular subject of interest. The present invention can be used to bring together content that is of particular interest to children on a single, self-contained network directed at children. The present invention can likewise be used to bring together content of particular interest to other target audiences, such as health-care providers, scientists, or persons working within a particular business sector. Bringing together this content on a self-contained network not only makes it easier to access this information, it also helps to build a sense of community among subscribers, who are likely to have similar interests.

Other features and advantages are disclosed in the specification below and in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 depicts the typical environment presented to children who login to the World Wide Web.

Figure 2 depicts one embodiment of a secure and safe internetworking system, as made in accordance with the principles with the present invention.

Figure 3 depicts one embodiment of a system for obtaining parental consent for allowing children to view certain material or any other situation requiring such consent.

Figure 4 depicts a chat room environment hosted on the presently claimed internetworking system, monitored in accordance with the principles of the present invention.

Figure 5 is a flowchart that implements one embodiment of a link monitor that oversees the request of content within the system.

Figure 6 is yet another embodiment of the link monitor that gives notification to parents that a child has requested unavailable material and gives an opportunity for parental

consent for loading the requested content onto the system.

Figure 7 is one embodiment of an address space for members that may be partitioned in a number of ways, including by age or parental consent.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to Figure 2, an embodiment of the internetworking system 200 as made in accordance with the principles of the present invention is shown. System 200 broadly comprises a stand-alone server 202 that connects with the outside world through ports 204. Child subscribers 206 would connect to server 200 in any number of ways known to those skilled in the art, including dial up modems to reach ports 204. Once connected to ports 204, server 202 would initiate logon procedure 208 to verify logon and account status.

If logon is complete, child 206 has access to a whole host of content that has been pre-selected for viewing by children and young adults. Such content might be in form of web pages (212, 216). Web pages themselves might be duplicates of web pages that already reside on the World Wide Web 100 that have been selected for their appropriateness for viewing by young people. All such web pages loaded onto server 202 is recorded in page registry 2 10, which comprises the addressable space of the system 200. Any request for a web page may be checked first in page registry 210 to see if the requested page has been loaded onto to server.

For example, web page 212 might comprise a hypertext link to another page 216. The request for page 216 would be checked in the page registry and its contents would be retrieved for download to the child's browser. Page 216 might contain a link to another page (Page X) which is currently not loaded onto the server 202; and, thus, any request for Page X would have to be denied.

Link monitor 220 would monitor the status of all requests for web pages or content in general. If a request is denied, link monitor 220 might perform a number of particular tasks. For example, link monitor 220 would inform the child that the requested page is not found on server 202. Additionally, link monitor 220 might inform the system administrator that a request has been denied. In our example, the system administrator might then look on the World Wide Web at Page X 222 and determine its appropriateness for viewing. If Page X is appropriate for all audiences, then the system administrator may load Page X onto server 202 for general viewing. If Page X is not appropriate for any audience on system 200, then the system administrator may choose to do nothing about Page X.

If, however, Page X is appropriate for viewing by young adults; but not by young children, then the system administrator may decide to make Page X available on server 202 to a selected subset of young viewers and not generally available. Alternatively, the system administrator might seek parental permission from the requesting child to load on Page X to server 202 and make available to the requesting child.

Figure 3 shows one embodiment of a system 300 for obtaining such parental consent. System 300 comprises a home computer 302 that is connected to system 200 as described above. Computer 302, at the time that system 200 is requesting the consent from parents, is running a parental consent form 304 that may describe the terms and condition of consent. This consent form is running concurrently with a finger print capture device 306 that captures the image of the parent's thumb print at the time the form is entered on screen. If the image data matches the thumb print information, possibly maintained on file with system 200 at the time the form is entered, then parental consent will be deemed given. It will be appreciated that other means of obtaining parental consent are possible, such as digital signatures, passwords, or voice recognition, and that the scope of the present invention should not be limited to any particular means.

Another feature of the present invention is depicted in Figure 4. System 200 may, in addition to hosting suitable content for young viewers, host a plurality of chat rooms 402 on the system. To increase the level of safety and security for the children on system 200, chat monitor 404 views all the posts placed by the children in chat room 402. As with the other prior art systems, any inappropriate post will invite with it a host of potential sanctions against the progenitor of the post. Chat monitor 404 is preferably accomplished by a human viewing the posts as they occur. However, automatic language filters may suffice as chat monitor either as a stand-alone facility, or in concert with a human overseeing the posts.

Additional security is provided the children by strictly limiting the number of children in any given chat room. In practice, the upper bound on the number of children in a chat room is ten; however, preferentially, the upper bound of children in any chat room is four. This upper bound provides a manageable level of children to monitor, as it has been known in the art that children tend to push the limits of chat rooms monitors in an effort to thwart built-in protections.

Figure 5 depicts one embodiment of the link monitor of the present invention that starts at step 502 monitoring the requests made by children (or members of the private internet) for content via a link in a pre-approved web page. Link monitor 500 would determine whether that particular link is within the existing address space of the system (i.e.

whether the content has been loaded onto the server). This determination might be made by a search with the registry to see if the link is currently there. It will be appreciated to those skilled in the art that the registry could be easily implemented in a data base or table format (or any other suitable data structure) for easy look-up. Thus, the scope of the present invention should not be limited to any particular implementation to the registry.

In another embodiment, the registry might comprise a compilations of verified child friendly sites, most up to date, and best (PG) sites available. This list might be categorized by age groups and subjects. Parents would have the option to select all of the material available or some of the content available depending upon what they deem suitable for their child.

If the link is within the registry, then the system would link would be provided to the child or member at 506 and displayed to the child/member's browser and the system would continue at 502.

If, however, the link is not within the registry at 504, then the link monitor may, as previously mentioned, might simply inform the child/member of the unavailability of the link. Alternatively, the link monitor might produce a work search within the current page at step 508 to provide a list of related links 510 to the child/member's browser at step 512 for possible selection. It will be appreciated that the system might already have, readily available, a list of alternative sites for a given link. Thus, the word search at step 508 might instead be a presentation of these pre-approved related sites.

Figure 6 is another embodiment of link monitor in which monitor 600 notes a child/members request for a link at step 602 and determines whether the requested link or content is within the registry (or otherwise available to the system) at step 604. If so, the requested page/link/content is sent to the child/member at step 606.

Otherwise, the child's parent (or member's system administrator) could be notified at step 608 of the unfulfilled request at step 608. If the parent or system administrator does not consent for that content to be viewed by the child or member, then the page/] ink/content is not loaded on the system for viewing by the child or member's browser at step 612.

If consent is granted by the parent or system administrator then such consent might be verified at step 614. Such verification might be garnered in any manner previously disclosed. For example, a request form might be presented -- describing the nature of the child or member's request -- to the parent or system administrator. At the same time, some form of verification might be requested simultaneously as the request is either granted or denied. The system depicted in Figure 3 whereby verification might be simultaneously requested via a fingerprint capturing system would suffice for the purposes of the present invention. Other

verification as previously discussed might also suffice.

If the consent is verified, then the page/content/link is made available to the child or member at step 618. In addition, the individual child or member's allowable address space might be updated to reflect the increased available content at step 620.

Figure 7 depicts one embodiment of a partitioning of allowable address space of either individual children/members or groups of children/members. The allowable content loaded onto the system might be more fine grained partitioned for access according to any number of parameter, including age as depicted in Figure 7. Age groups 702 -- shown here as ages 0-5 (704), ages 6-10 (706), or ages 11-18 (708) -- might be allowable address spaces for children as they initiate access to materials. As children make request for materials beyond their current classification, the children might ask either parents or system administrator for increased levels of access at 712. This process might proceed as previously described for access to content. Parents might ask the system administrator at step 714 to either add material specific to the child or to increase the age grouping for that particular child.

It will be appreciated that age is just one of many possible metrics for the partitioning of the content address space for its children or members of a private internet. Other suitable metrics might include allowable interests, need-to-know status, or any other appropriate partitioning metric. The scope of the present invention encompasses the various possible metrics and that the scope should not be limited to those shown in the figures.

CLAIMS

1. An internetworking system for providing a safe and secure environment for its members, said system comprising:

a server system;

a plurality of input ports connected to said server system; a plurality of pre-selected web pages, said web pages selected to be appropriate for its members and wherein said web pages comprise zero or more hypertext links to other pages;

a registry of all pre-selected web pages, said registry defining the address space of said system;

a login procedure whereby a member possessing an account on said internetworking system connects with an input port and said member supplies sufficient information to verify said member's account;

a link monitor whereby a hypertext link request from a member via a web page currently viewed by said member is compared with said registry to determine whether said requested web page is within the address space of the system.

2. The internetworking system as recited in Claim 1 wherein said link monitor alerts the member that a requested page is not loaded onto said system.

3. The internetworking system as recited in Claim 1 wherein said link monitor alerts the administrator that certain material requested by said member was not loaded on said system.

4. The internetworking system as recited in Claim 3 wherein said link monitor queries said administrator for consent for loading requested material not found or the system and for allowing their member to view said material.

5. The internetworking system as recited in Claim 4 wherein said consent is obtained by inputting verification data of said administrator while, concurrently, a consent form is entered into said system.

6. The internetworking system as recited in Claim 5 wherein the verification data is the fingerprint image digitally captured.

7. The internetworking system as recited in Claim 5 wherein the verification data is a speech recognition pattern.

8. The internetworking system as recited in Claim 5 wherein the verification data is a digital signature.

9. The internetworking system as recited in Claim I wherein said system further comprises:

a chat room whereby members logged onto to said system may engage In real time conversation,

a chat monitor wherein said monitor oversees the conversation occurring in said chat room for the appropriateness of the conversation taking place.

10. The internetworking system as recited in Claim 9 wherein said chat room is limited to an upper bound on the number of members allowed to enter the chat room at any given time.

11. The internetworking system as recited in Claim 10 wherein said upper bound of members allowed at any given time in a chat room is ten members.

12. The internetworking system as recited in Claim 10 wherein said upper bound of members allowed at any given time in a chat room is four members.

13. The internetworking system as recited in Claim 2 wherein said system presents to the member a list of related sites to connect to in lieu of the unavailable site requested.

14. The internetworking system as recited in Claim 13 wherein said system performs a word search within said current page to determine a list of related sites to present to the member.

15. The internetworking system as recited in Claim 1 wherein said address space of allowable content is partitioned for individual members according to a given parameter.

16. The internetworking system as recited in Claim 15 wherein said partitioning parameter is the age of the member.

17. The internetworking system as recited in Claim 15 wherein said partitioning parameter is the allowable interest of the member.

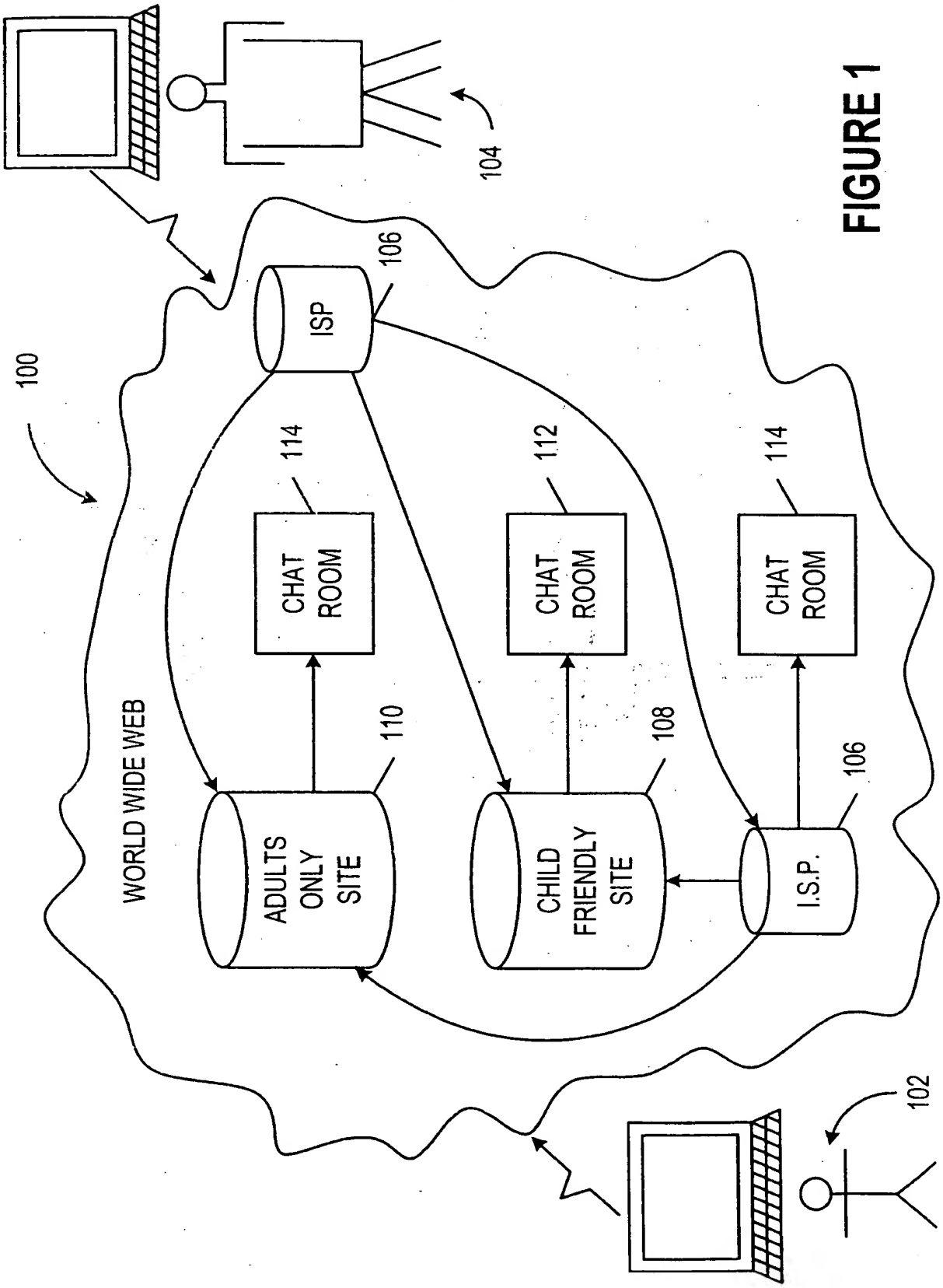

104
100
ISP
106
114
112
114
CHAT ROOM
CHAT ROOM
CHAT ROOM
WORLD WIDE WEB
110
108
106
ADULTS ONLY SITE
CHILD FRIENDLY SITE
I.S.P.
102

FIGURE 1

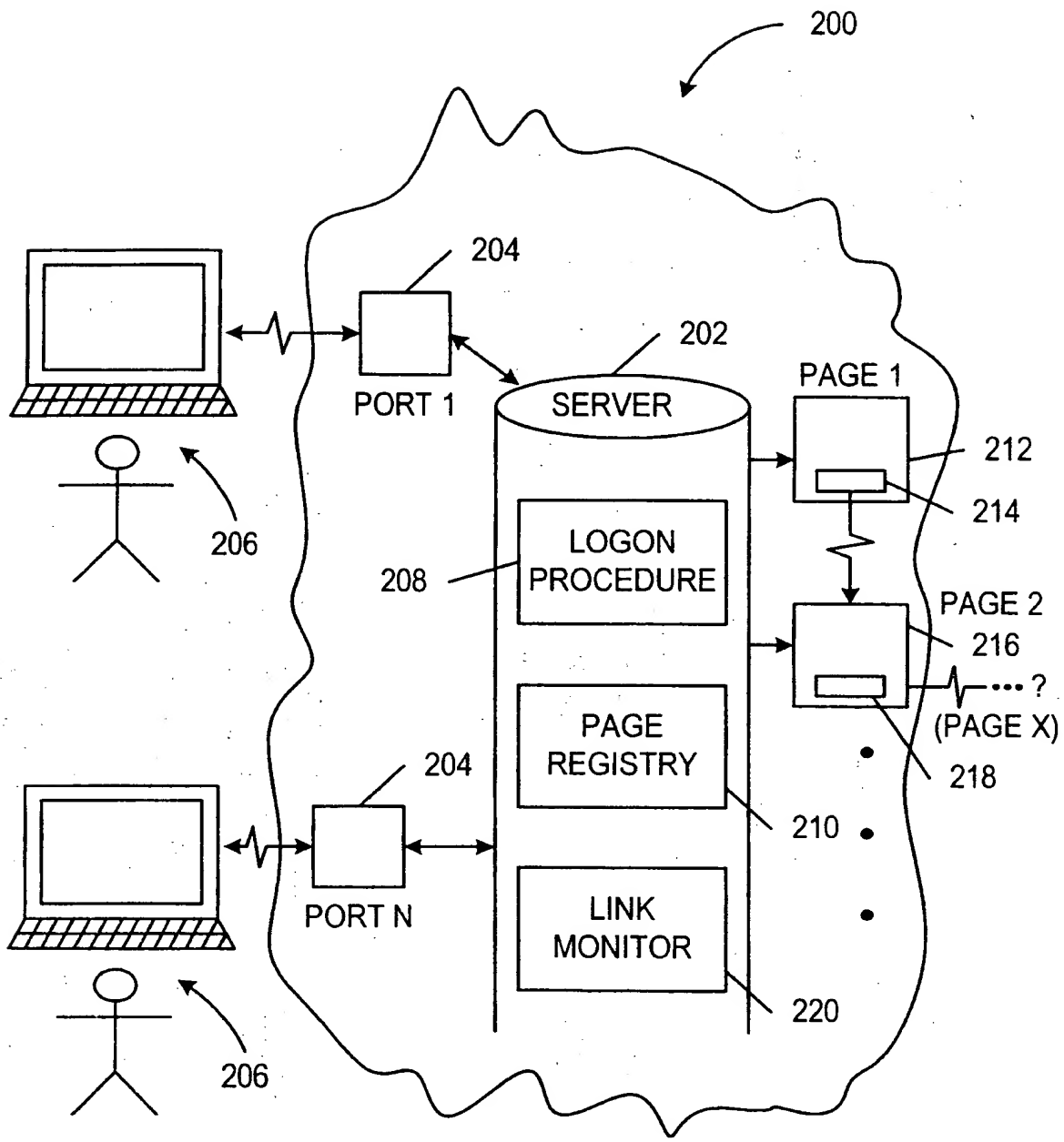

200
204
202
PORT 1
SERVER
PAGE 1
212
214
206
LOGON PROCEDURE
208
PAGE 2
216
? (PAGE X)
PAGE REGISTRY
218
204
210
PORT N
LINK MONITOR
220
206

FIGURE 2A

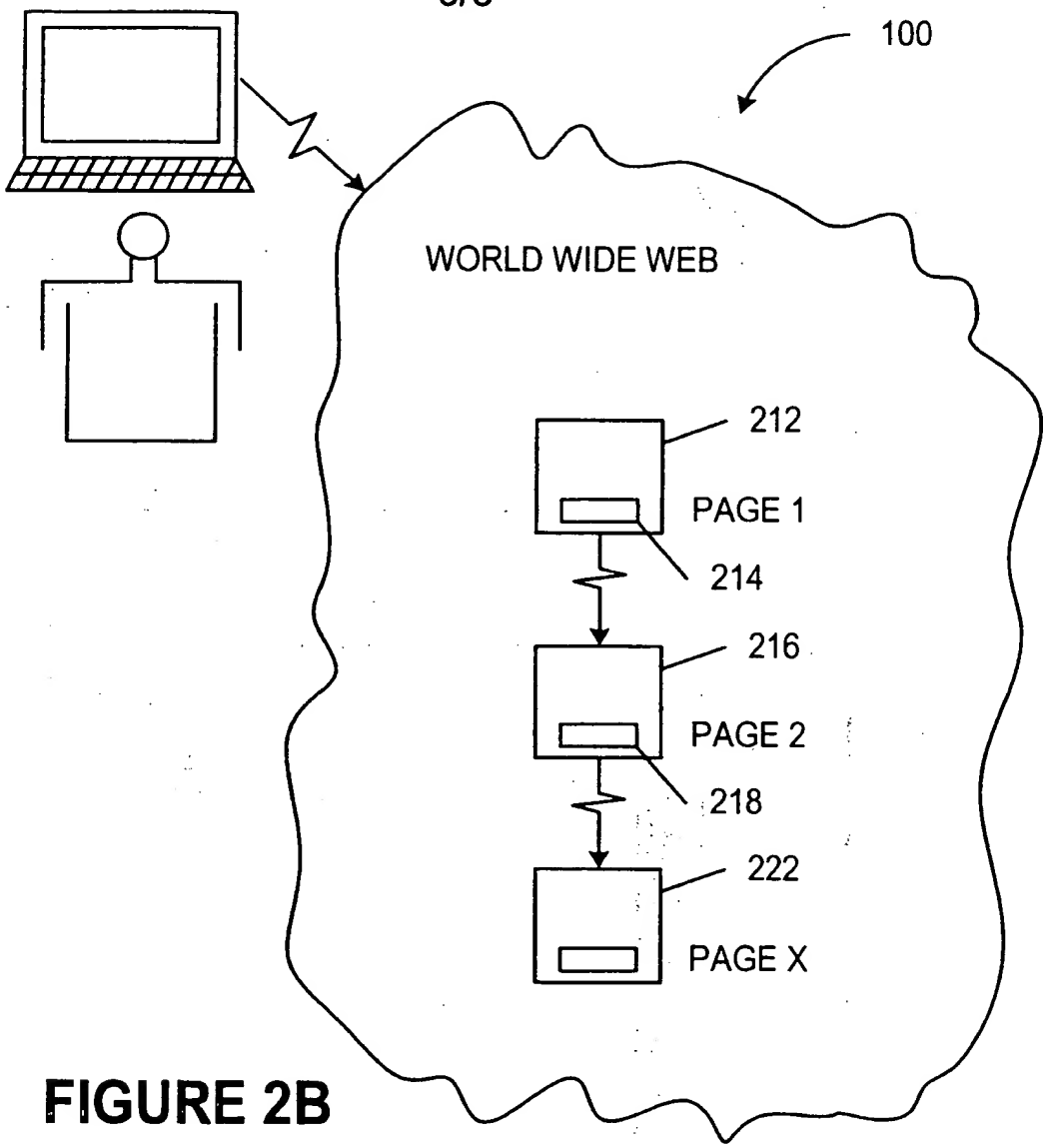


FIGURE 2B

FIGURE 2A	FIGURE 2B

FIGURE 2

FIGURE 3

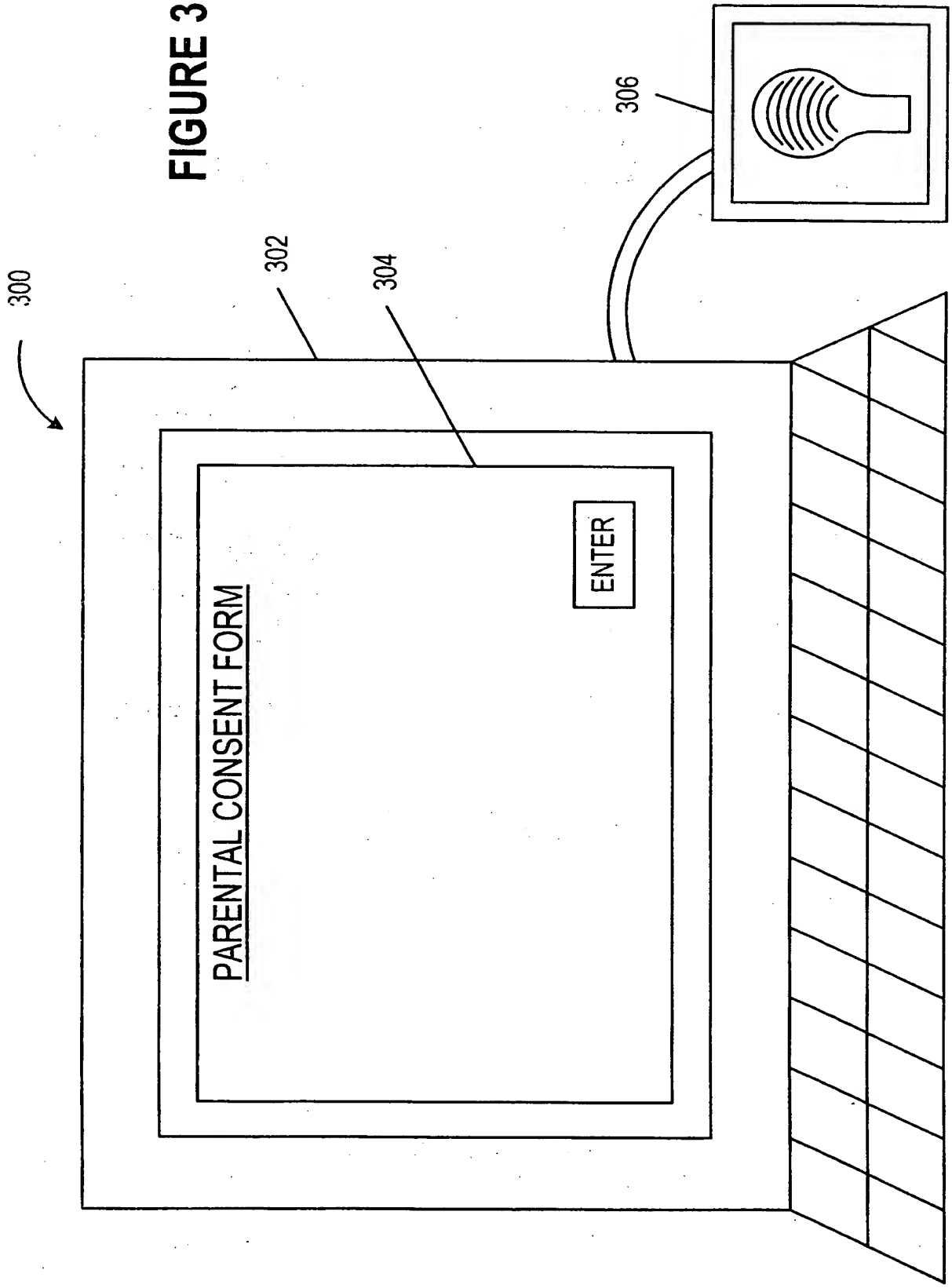
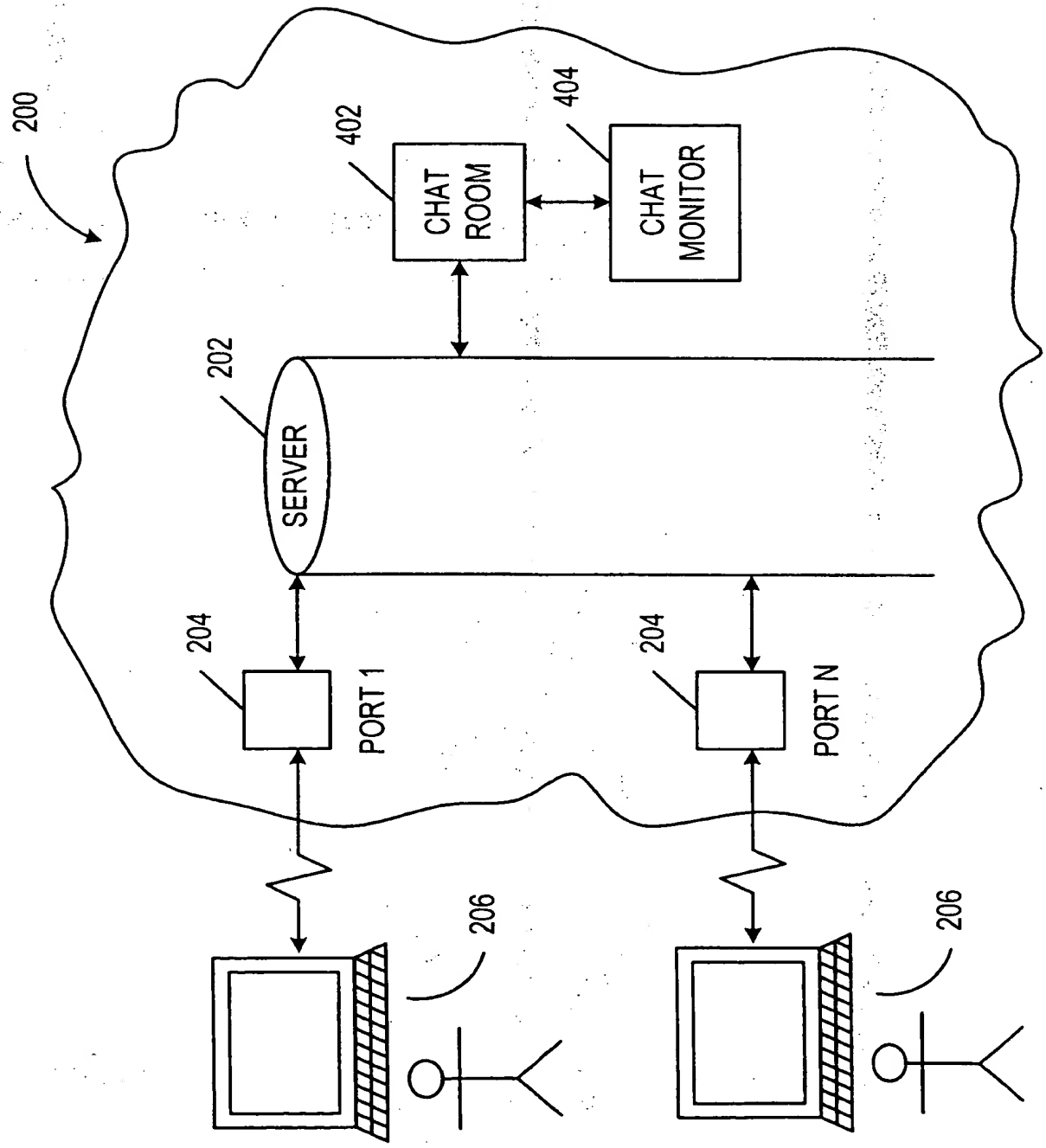


FIGURE 4



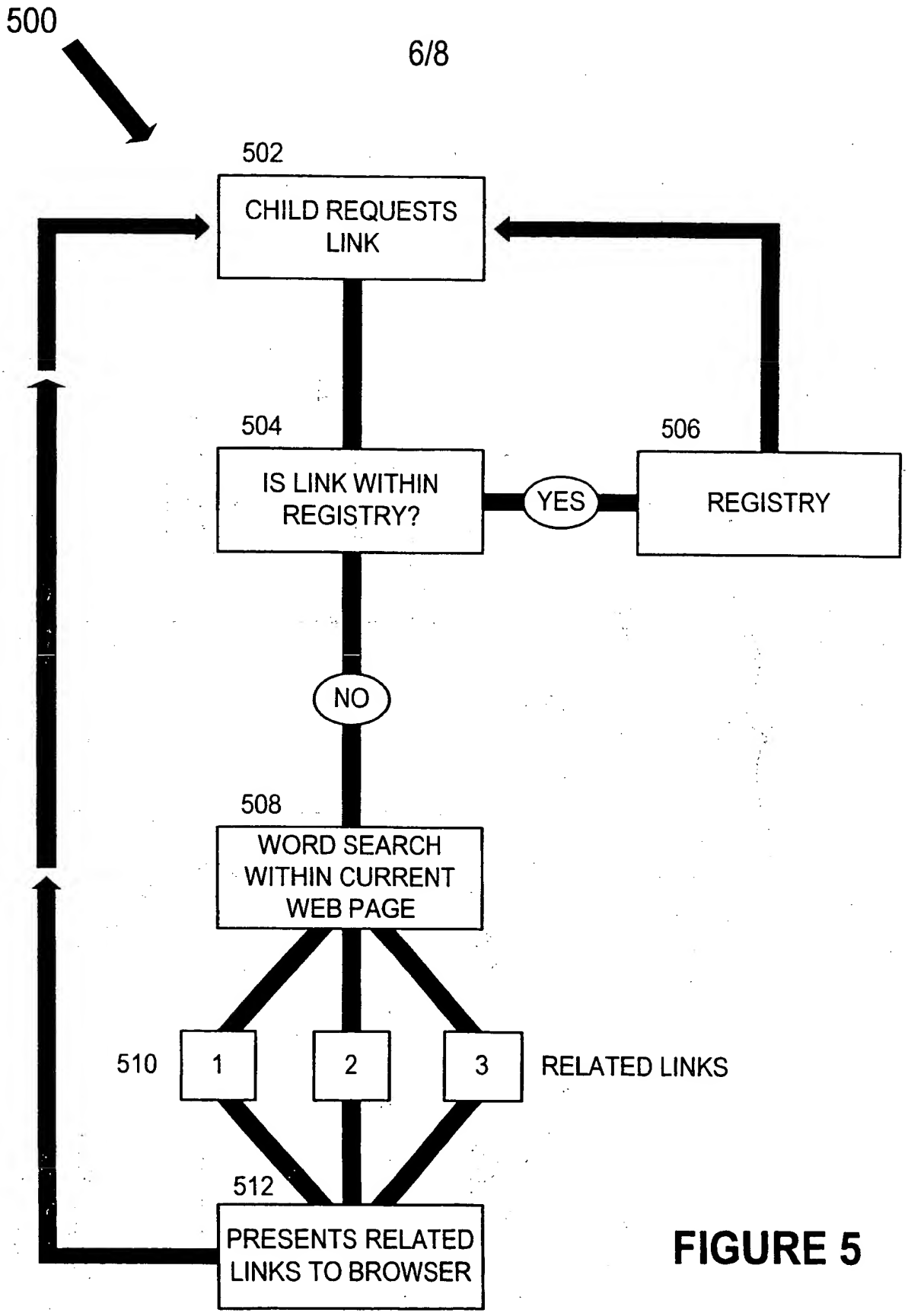
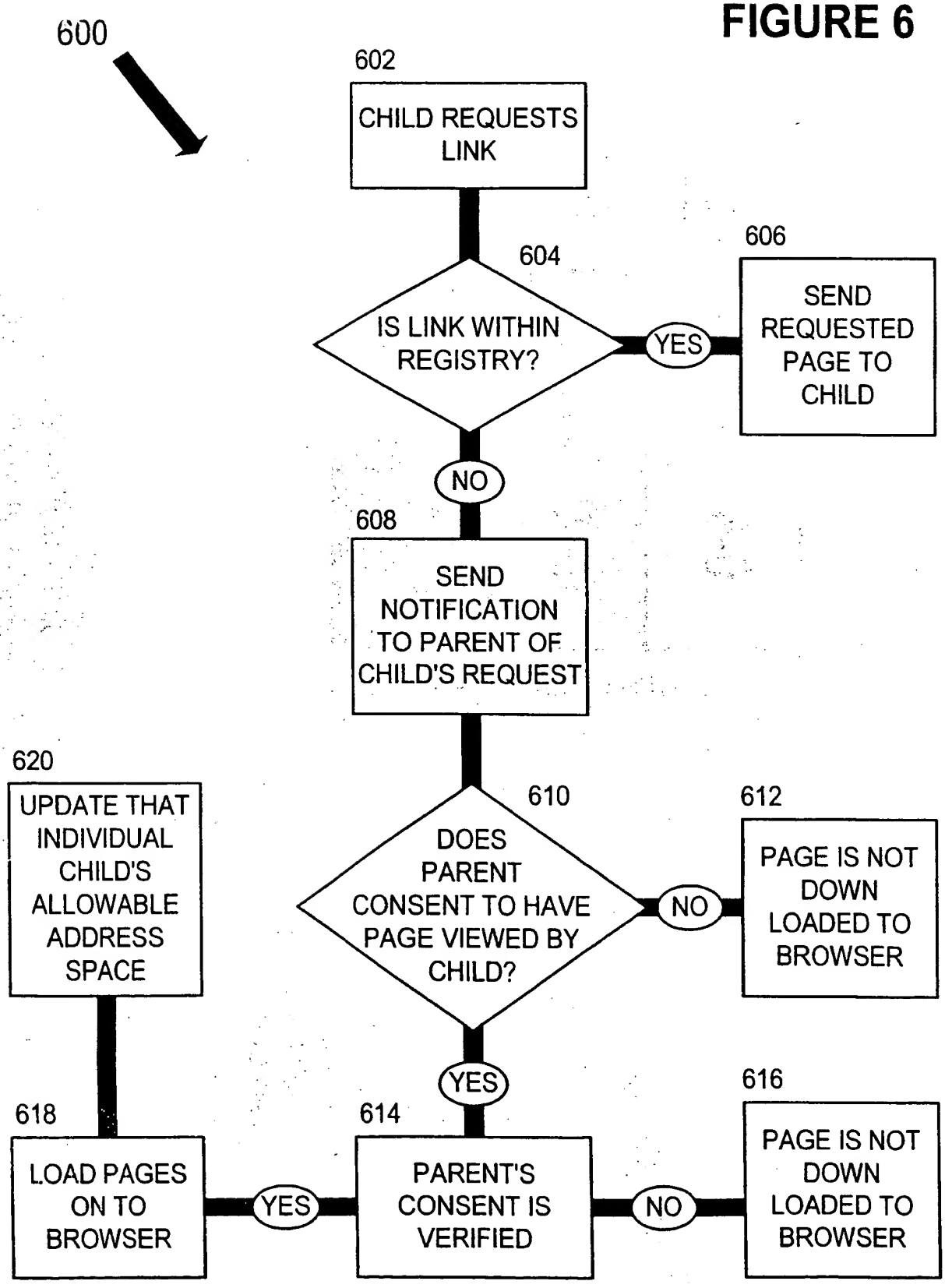


FIGURE 5

FIGURE 6


600
602
CHILD REQUESTS LINK
604
IS LINK WITHIN REGISTRY?
YES
606
SEND REQUESTED PAGE TO CHILD
NO
608
SEND NOTIFICATION TO PARENT OF CHILD'S REQUEST
610
DOES PARENT CONSENT TO HAVE PAGE VIEWED BY CHILD?
NO
612
PAGE IS NOT DOWN LOADED TO BROWSER
YES
614
PARENT'S CONSENT IS VERIFIED
NO
616
PAGE IS NOT DOWN LOADED TO BROWSER
YES
618
LOAD PAGES ON TO BROWSER
620
UPDATE THAT INDIVIDUAL CHILD'S ALLOWABLE ADDRESS SPACE

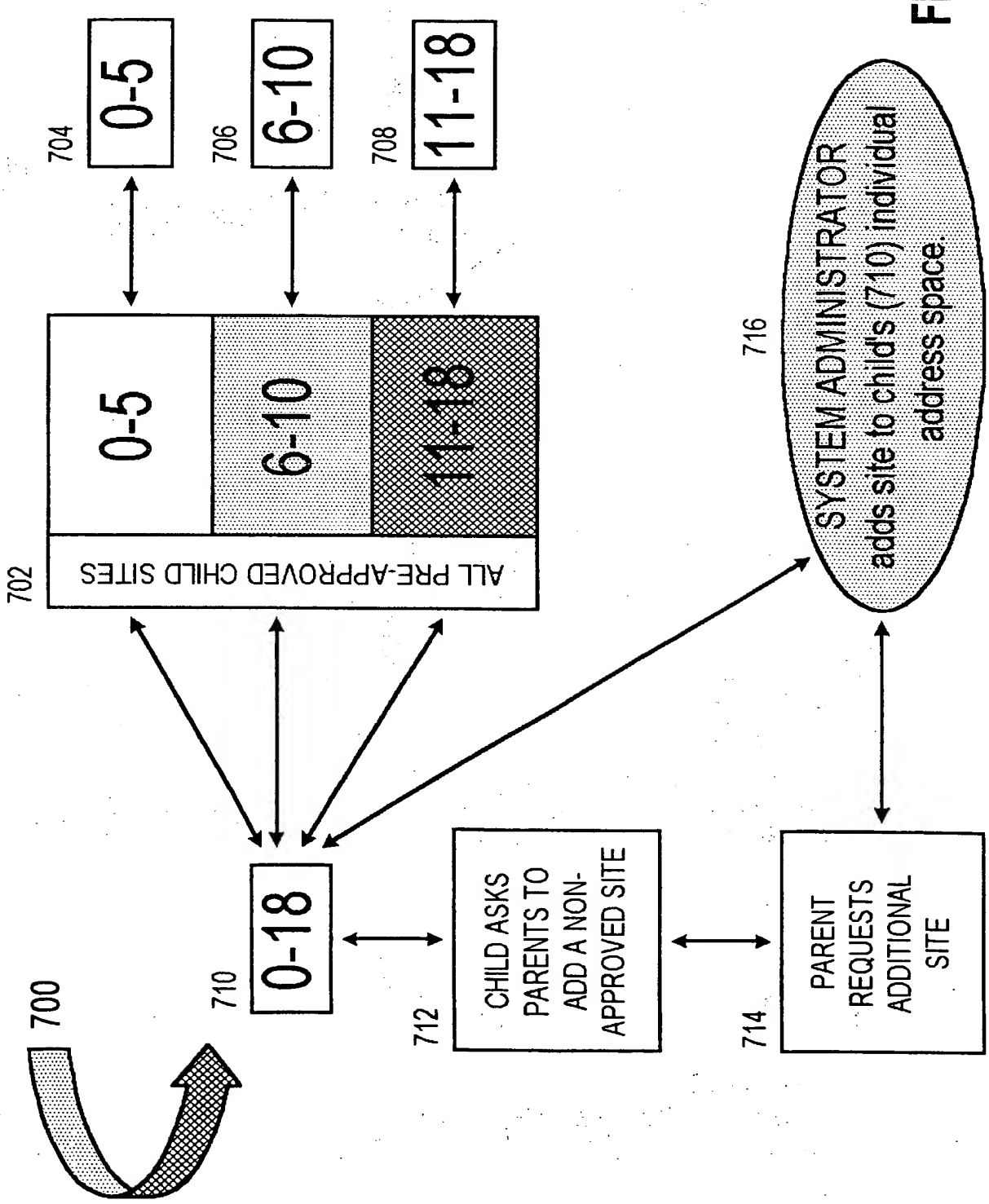


FIGURE 7

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 November 2000 (09.11.2000)

PCT

(10) International Publication Number
WO 00/67096 A3

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US00/11997

(22) International Filing Date: 3 May 2000 (03.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/304,245 3 May 1999 (03.05.1999) US

(71) Applicant and
(72) Inventor: CALAMARI-LINDQUIST, Eleanor (aka ST. JOHN, El) [US/US]; Silvertech Inc., Suite 103, 1415 Indiana Street, San Francisco, CA 94107 (US).

(74) Agents: CASERZA, Stephen, F. et al.; Flehr Hohbach Test Albritton & Herbert LLP, Suite 3400, 4 Embarcadero Center, San Francisco, CA 94111 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

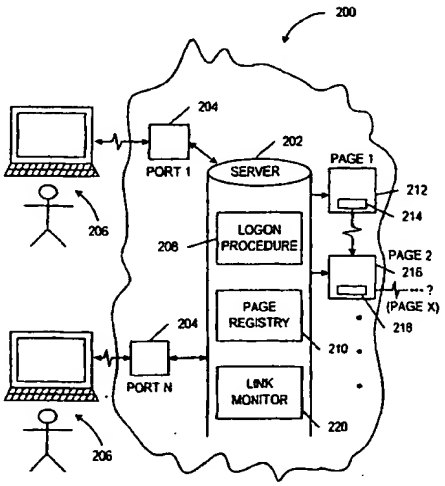
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

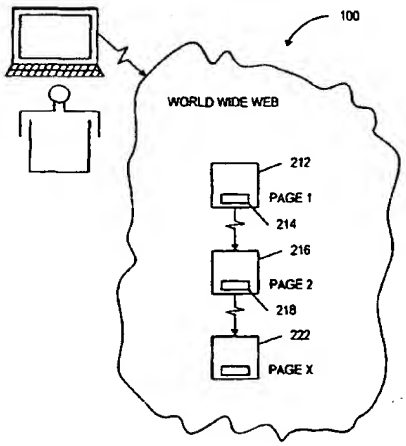
Published:
— *With international search report.*

(88) Date of publication of the international search report:
31 May 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SUPERVISED INTERNET ACCESS





(57) Abstract: A system is presented for providing a secure and safe internetworking system that is a completely self-contained internet exclusively for children or other private groups. The system comprises a server system, a plurality of dial-up ports connected to said server system, and a plurality of web pages comprising content that is suitable for children or other private groups. The address space of content loaded onto the system may be partitioned for individual children or member and may be increased by authenticated, verified consent by parents or system administrators. The system provides hardware and/or means for authorizing the addition of requested web pages onto the system. In another aspect of the present invention, there is an upper limit imposed on the number of children engaged in any particular chat room. Chat among children is monitored either by humans or automatic language filters whereby the number of children in a given chat room does not exceed a pre-set upper bound.

WO 00/67096 A3

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 00/11997

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 696 898 A (GROSSE ERIC ET AL) 9 December 1997 (1997-12-09) column 1, line 10 -column 2, line 20 abstract	1
A		2-17

A	US 5 706 507 A (SCHLOSS ROBERT JEFFREY) 6 January 1998 (1998-01-06) abstract	1-17

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 December 2000	12/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Canosa Aresté, C

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/US 00/11997

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5696898 A	09-12-1997	CA 2196867 A	07-12-1996
		CN 1159234 A	10-09-1997
		EP 0793826 A	10-09-1997
		WO 9715008 A	24-04-1997
US 5706507 A	06-01-1998	NONE	